The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 8 April 13, 2016

ENFORCEMENT ACTIONS

Ten Steps to Minimize Data Privacy and Security Risk and Maximize Compliance

By Aaron Charfoos, Jonathan Feld and Stephen Tupper
Dykema

Increasingly, general counsel, privacy officers and even CEOs are taking on more and more data privacy and security compliance burdens because of the significant legal implications of not just breaches, but failure to comply with a range of privacy and cybersecurity regulations. That applies to international transfers of data as well. In this article we discuss recent global developments and ten ways companies can ensure compliance with new regulations to increase data security and minimize the risk of enforcement actions.

U.S. Privacy and Cybersecurity Trends

In the U.S., the main theme seems to be enforcement, as the year began with several announcements that could mean aggressive federal privacy and cybersecurity actions.

FTC as Major Privacy Enforcer

In the FTC's report on Big Data, "Big Data – Tool for Inclusion or Exclusion," the agency continues to assert that it has broad data protection powers under the Fair Credit Reporting Act despite some setbacks last year.

This announcement comes on the heels of settlements by the FTC in the Wyndham and AsusTek cases over allegations that both companies engaged in deceptive and unfair trade practices. See "*In the Wyndham Case, the Third Circuit Gives the FTC a Green Light to Regulate Cybersecurity Practices*" (Aug. 26, 2015).

In addition, by taking a prominent role in the enforcement of the E.U.-U.S. Privacy Shield, discussed below, the FTC seems to have solidified its role as the major privacy enforcer in the U.S.

SEC and CFPB Asserting Powers

Numerous other federal agencies are asserting their powers as well. This year's SEC Enforcement Priorities list specifically called for a focus on cybersecurity controls by broker-dealers and investment advisers. See "*The SEC's Updated Cybersecurity Guidance Urges Program Assessments*" (May 6, 2015).

In a somewhat surprising move, the Consumer Financial Protection Bureau (CFPB) announced that it had reached a consent decree with Dwolla, Inc. What made the announcement notable was not simply that the CFPB was now moving aggressively into the privacy space, but that it had commenced the action even though no breach had occurred. This demonstrates that agencies have expanded their focus to protecting consumers prior to a breach.

European Privacy and Cybersecurity Trends

In Europe, the key theme so far in 2016 and going forward is new or revised regulation.

GDPR Centralizes Data Privacy

At the end of 2015, the European Union took another step closer to enacting a General Data Protection Regulation (GDPR) to govern how all data in Europe should be treated. This is likely to be passed into law this year. The GDPR will replace a more decentralized scheme that has been in place since 1995 with a comprehensive, mostly "one-stop shop" for privacy rules.

The GDPR, like its predecessor law, protects "personal data" which is broadly defined to include "any information relating to an identified or

identifiable natural person" and will place broad obligations on controllers and processors of data to protect data throughout its entire life cycle. The GDPR will become effective two years after its anticipated 2016 enactment.

Although two years sounds like a lot of time, the depth and breadth of the additional requirements will result in lots of preparation by enterprises that do business in Europe or that move personal data about European citizens. Work to achieve compliance will involve new contracts, internal procedures, revisions to privacy policies and statements and other activities. There is no time to waste.

See "*The E.U.'s New Rules: Latham & Watkins Partner Gail Crawford Discusses the Network Information Security Directive and the General Data Protection Regulation*" (Jan. 20, 2016).

Privacy Shield Replaces Safe Harbor

At the same time, the European Court of Justice (ECJ) struck down the so-called Safe Harbor arrangement that had previously allowed thousands of U.S. businesses to move information from Europe to the U.S. In the wake of this decision, E.U. and U.S. negotiators have developed a new framework, called the E.U.-U.S. Privacy Shield, to replace the Safe Harbor and provide a similar mechanism to permit transfers. The U.S. Department of Commerce and other U.S. government agencies released their proposed structure for the Privacy Shield in February 2016.

Like the prior Safe Harbor, the framework governs the steps a U.S. organization needs to take in order to ensure that any data moving out of the E.U. is properly protected once it lands in the U.S. The Privacy Shield once again relies on self-certification, but is far more stringent in terms of notice, consent, recertification, adopting efficient mechanisms to raise privacy concerns by E.U. citizens and oversight by relevant U.S. governmental agencies.

In addition, the Privacy Shield addresses concerns about surveillance by the U.S. government itself. The framework will need a number of approvals before it becomes enforceable but European commissioners have publicly stated that they believe it will become effective by June 2016. Although U.S. enterprises that were self-certified under the Safe Harbor will have a head start on moving to the Privacy Shield regime, the change will mean more than just changes to policies and certifications. As with GDPR compliance, enterprises will need to give themselves sufficient time to ensure that they are prepared for the new rules.

See also "*Deal Struck to Maintain the Transatlantic Data Flow*" (Feb. 17, 2016).

Ten Steps to Minimize Risk and Maximize Compliance

Below are the steps that enterprises should be taking in 2016 to minimize the risk of enforcement actions and ensure compliance with the new regulations.

1) Get to Know Your Data. Really Well.

The first step is to fully understand what information is collected, how it is used, how it is protected, with whom it is shared, and how long it is kept. It also matters where data moves as national and international law increasingly deals with data transfers. Many organizations' compliance regimes were created for a traditional IT model where data resided on the enterprise's own servers behind the enterprise's own firewall.

Today, while those legacy systems may remain, vast amounts of data are stored in the cloud in virtual instances of servers that are spread around the globe. In addition, employees are traveling globally with laptops, smartphones and tablets that are communicating back with the organization. This new reality requires an entirely different way to protect that data, both physically and legally.

Creating and maintaining data inventories and data flows are critical to staying on top of this evolving landscape.

See also "*How to Reduce the Cybersecurity Risks of Bring Your Own Device Policies (Part One of Two)*" (Oct. 14, 2015); Part Two (Nov. 11, 2015).

2) Understand Your Legal and Regulatory Landscape

A company's headquarters may be in Chicago but its data may flow across the globe subjecting it to many different legal regimes. As discussed above, on the one hand, Europe appears poised to enact an E.U.-level and data protection regime that avoids much of the need to work through regulations of the different member states.

On the other hand, the U.S. has adopted a sectoral approach and continues to be governed by a patchwork of laws and agencies. Organizations must be aware of regulations in the financial (e.g., the Gramm-Leach Bliley Act and the Fair Credit Reporting Act), healthcare (e.g., HIPAA and the HITECH Act), education (e.g., the Family Educational Rights and Privacy Act), and other areas at the federal level.

At the state level, most states have data security, breach notification, and other consumer protection regulations. Many states have also enacted their own privacy and data protection laws. For example, California has an information security statute that legally requires businesses to use "reasonable security procedures and practices…to protect personal information" and Illinois has a law preventing the unauthorized use of biometric information. In addition, certain industry groups have their own sets of regulations (e.g., the Payment Card Industry Data Security Standard, or "PCI DSS," for payment card transactions).

With so many players, it is very easy for any enterprise to stray into regulated space. Therefore, enterprises must regularly identify what laws and regulations apply, what they require and be constantly vigilant as they change over time.

3) Verify That Your Data Transfers Comply With the Relevant Law

Once an enterprise has identified its data flows, the next step is to verify that each flow that crosses an international boundary is authorized (or at least is not prohibited). All European Economic Area (EAA) countries, as well as other countries like Australia, Israel and the United Arab Emirates, require that certain protections follow the data when it is transferred to another nation. And even something as simple as accessing the enterprise directory for an enterprise's e-mail system (like Active Directory for Microsoft Outlook) can count as a transfer. Many enterprises identify the source and destination countries, then identify the bases upon which they are legally transferring the personal data.

Means of legally transferring data can include circumstances where there is:

- no prohibition on the transfers out of the country;
- fully-informed consent of the data subject;
- a nationally-recognized program like the U.S. Safe Harbor used to be and the new U.S. Privacy Shield is expected to be;
- use of approved contractual arrangements, such as the European Commission's approved "Standard Contractual Clauses," whether using individual sets of clauses between entities or embedding the clauses in an enterprise-wide data transfer agreement that covers all entities in the enterprise;
- use of "binding corporate rules" or "BCRs," which amount to intra-enterprise rules approved by two or more European data protection authorities (an intensive process that has produced only 86 approved enterprises, mostly in the information technology, finance, and pharmaceutical industries); or
- a narrow exception in the law, such as performance under contracts.

See also "*Making Sense of Cybersecurity and Privacy Developments in the E.U.*" (Mar. 16, 2016).

4) Know Your Privacy Statements

It is not uncommon for enterprises to have a number of different internal privacy policies and external privacy statements. Enterprises should regularly review their privacy statements and policies to ensure that they accurately reflect the enterprise's business and are consistent with any relevant laws.

Given the worldwide reach of enterprises and websites, it is often necessary to have sections of a single policy targeted to different geographic regions. For example, California's privacy policy requirements differ significantly from those that are currently included in the new E.U.-U.S. Privacy Shield. Having a section of the policy devoted to California citizens and a different section devoted to European citizens will ensure compliance with both. Of course, the enterprise's compliance regime will also need to ensure compliance with all of these policies.

5) Secure Consent

This is often overlooked, but obtaining consent from data subjects can be a useful tool for enterprises. The first step is to understand which users can and should give consent, and which ones do not need to. Then, enterprises should ensure that the consent is effective. A common reason that consent becomes ineffective is that the privacy statements and notices become stale and do not reflect the evolution of the enterprise's business or products.

6) Ensure Certifications Are Up to Date

Many enterprises rely on certifications to both attract customers and reduce their legal risk. But enterprises must keep those certifications up to date. Over 4,000 U.S. enterprises used to transmit data out of the E.U. under the U.S. Safe Harbor. As discussed, the Safe Harbor was invalidated by the ECJ last year and no longer provides any benefit to those enterprises (even though many enterprises still include information about the now defunct Safe Harbor on their websites) and likely will not provide much benefit for the new Privacy Shield self-certification process. Moreover, many certifications need to be renewed or require periodic compliance checks. In order to obtain the maximum benefit from the certification, enterprises should ensure that they are keeping them current and following all of the necessary rules.

7) Be Careful What You Promise

Several recent enforcement actions brought by the FTC (after a reported breach) and CFPB (before any breach had occurred) emphasize that enterprises must be very careful what they promise their customers. In each instance, statements made by the enterprise about the security of their products or the safety of the data they held were alleged to be deceptive or unfair because they did not allegedly accurately reflect the risks to the personal information held by the enterprise. These statements are likely some of the most difficult to police, but pose some of the greatest enforcement risk. To be sure, to the extent that any vulnerabilities are actually discovered, enterprises should also review their marketing materials to ensure that there are no promises that are now inaccurate.

See also "*A Behind-the-Curtains View of FTC Security and Privacy Expectations*" (Mar. 16, 2016).

8) Strengthen Technical Safeguards

While many laws and regulations do not require any particular technical requirements, some do. California's Attorney General recently released a report that publicly stated that the failure to adopt the Center for Internet Security's Critical Security Controls as a minimum level of security constitutes a "lack of reasonable security" as required by California law. Similarly many industry standards, such as PCI DSS, include stringent technical requirements. Chief privacy or information security officers, in-house counsel and others will need to work closely with the enterprise's technical team and vendors to ensure compliance.

See "*Coordinating Legal and Security Teams in the Current Cybersecurity Landscape" Part One* (Jul. 1, 2015); *Part Two* (Jul. 15, 2015).

9) Implement a Breach Response Plan

The process of dealing with a data breach should begin long before the breach occurs. The U.S. alone has more than 45 separate state data breach notification laws and the minutes or hours after discovery of a breach are not the time to begin to determine what those are. Now is the time to make sure that your response plan accurately reflects the technical reality of the organization, as well as complies with all of the new changes in the law. The plan should be well-defined, written down and accessible to all of the key players in the event of a data breach. In addition, enterprises should prescreen all of the key partners necessary in the event of a breach including qualified outside legal counsel, technical data breach response experts, public relations firms and others.

See also "*Proactive Steps to Protect Your Company in Anticipation of Future Data Security Litigation (Part One of Two)*" (Nov. 25, 2015); *Part Two* (Dec. 9, 2015).

10) Perform Data Breach Drills

Enterprises should also run mock data breach drills to ensure that the plan can be implemented as drafted. These mock drills can range from tabletop exercises to full blown all-hands-on-deck scenarios. The key is to ensure that all of the pieces are in place for a competent, efficient and manageable response to the breach. Here, outside counsel can be particularly helpful in developing and running the drill and protecting it with the cloak of privilege (in some countries, such a privilege does not attach to communications involving in house counsel). An organization's well-rehearsed response to a breach may play a key role in defending against any future litigation or enforcement actions.

Aaron Charfoos is a member in Dykema's privacy, data security and e-commerce practice and is an experienced trial lawyer specializing in complex patent, privacy and data protection litigation and counseling. Jonathan S. Feld is the leader of the government investigations and corporate compliance team. Mr. Feld's practice focuses on complex civil and criminal matters, including antitrust, health care, financial and anti-bribery actions. Stephen Tupper is the leader of the firm's privacy, data security, and e-commerce practice. He focuses on information technology, outsourcing, electronic commerce, technology development and licensing, privacy and general corporate law matters.